CHECKLIST: HOW TO STOP RANSOMWARE IN ITS TRACKS

Key Technologies

Despite rumors of its demise, ransomware continues to be one of the top cyber threats facing organizations, with 30% admitting to have been victimized in the past[1]. It is therefore critical that you have advanced protection technologies in place to keep your organization secure.

Stop Attacks From Getting Into and Spreading Within Your Network

Stopping ransomware from entering and spreading within your network is vital. This can be achieved with a next-generation firewall. Look for the following key features when evaluating solutions:

☐ Top performing IPS (Intrusion Prevention System) engine

A modern, high-performance IPS engine is a critical security component of any next-gen firewall, as it performs deep packet inspection of network traffic to identify vulnerability exploits and block them before they reach a target host.

☐ Lockdown Remote Desktop Protocol (RDP)

Your firewall should enable you to easily restrict access to VPN users and whitelist sanctioned IP addresses.

☐ Sandboxing Technology

Your firewall should incorporate sandboxing technology to ensure all suspicious active files coming in through web downloads and as email attachments are being suitably analyzed for malicious behavior before they get onto your network.

☐ Zone Segmentation

Your firewall should enable you to reduce lateral movement within the network by segmenting LANs into smaller, isolated zones or virtual LANs secured and connected by the firewall.

☐ Application Identification and Control

Your firewall should enable you to identify and restrict which applications can run on the network, and block those typically used in ransomware attacks.

Securing Your Endpoints and Servers

Stopping ransomware from gaining a foothold on your endpoints and servers is vital. Look for the following key features in your endpoint and server protection solution:

☐ Anti-ransomware Technology

Your solution should secure your endpoints with technology specifically designed to detect and stop ransomware. It should be able to identify ransomware behaviour by blocking malicious encryption that attempts to make unauthorized changes to your data. The technology should also:

- Work against both local and remote encryption
- Stop both file-based and full disk ransomware
- Automatically roll back changes to files with no loss of data

☐ Exploit Prevention

Attackers take advantage of vulnerabilities in other software products in order to distribute and install ransomware. Exploit prevention technology stops the techniques attackers rely on to achieve their goals.

☐ Machine Learning

Your solution should be able to utilize deep learning, or other machine learning techniques, to analyze the "DNA" of files and block never-seen-before ransomware before it can execute.

☐ HIPS Behavior Analysis/File Analytics

Your endpoint solution should be able to examine the components/structure of files for malicious elements and checks if it contains code trying to modify the registry.

SOPHOS

☐ Web Security and Malicious Traffic Detection

Your solution should search for malicious code and block access to exploit landing pages.

☐ Device Control

Your endpoint solution should be capable of restricting removable media access such as USB keys to eliminate the risk of infected media.

☐ Managed Detection and Response (MDR)

Your solution provider should be able to complement your endpoint solution with a 24/7 monitoring and response service. MDR services hunt for and investigate suspicious activity and potential indicators of compromise that might expose your organization to ransomware attacks.

Stop Phishing Emails

Phishing emails are one of the most common attack vectors for ransomware. Make sure your users are prepared:

☐ Simulated Phishing Attacks

Tests the preparedness of your organization against targeted phishing campaigns.

☐ Customizable Phishing Campaigns

Match the content of the emails to your organization and industry – carefully localized for multiple languages. For example, run a campaign on HIPAA compliance and train your users on suspicious things to look out for.

☐ Detailed Insight into User Performance

Identify how many users failed, how susceptible they are to phishing attacks, average training passing scores, and more.

How Sophos Helps Keep You Secure

Stopping attacks get into network

Sophos XG Firewall is packed with technology to help protect your organization from ever-evolving ransomware attacks. In particular, XG Firewall includes one of the best performing and most effective IPS engines on the market, and provides a simple and elegant solution to lockdown your RDP servers.

XG Firewall offers flexible and easy segmentation tools like zones and VLANs to secure your LAN and reduce the risk of lateral movement, reducing surface area of attack and minimizing the risk and potential scope of propagation.

Securing your endpoints and protecting your servers

Should hackers somehow access your network, Intercept X uses multiple layers of defense to stop ransomware in its tracks. Anti-exploit technology stops the delivery of ransomware, deep learning blocks ransomware before it can run, and CryptoGuard prevents the malicious encryption of files, rolling them back to their safe state. The endpoint detection and response (EDR) functionality within Intercept X additionally detects advanced ransomware attacks that may have gone unnoticed and search for indicators of compromise across your network.

Furthermore, Sophos Managed Threat Response (MTR enables 24/7 threat response actions to be identified and executed utilizing a fusion of machine and human intelligence.

Educating on phishing techniques

Sophos Phish Threat sends simulated phishing attacks to your organization, testing preparedness against real world attacks. Emails can be customized to your organization and industry and have been carefully localized for multiple languages. Detailed feedback lets you see how many users failed, overall susceptibility to attacks, and more.

1 The Impossible Puzzle of Cybersecurity

Try XG Firewall for Free at sophos.com/xg-firewall	Try Intercept X for Free at sophos.com/intercept-x	Try Phish Threat for Free at sophos.com/phish-threat

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North America Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

SOPHOS

2019-10-07 CL-NA (NP)